

PCT/JP 03/14517

14.11.03

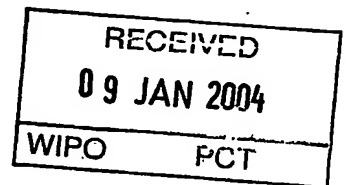
日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2 0 0 2 年 1 1 月 1 5 日

出 願 番 号  
Application Number: 特 願 2 0 0 2 - 3 3 1 8 8 4  
[ST. 10/C]: [ J P 2 0 0 2 - 3 3 1 8 8 4 ]



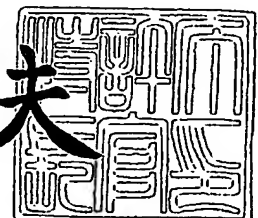
出 願 人  
Applicant(s): 三洋電機株式会社  
株式会社数理設計研究所  
三洋セミコンデバイス株式会社

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2 0 0 3 年 1 2 月 1 8 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



CERTIFIED COPY OF  
PRIORITY DOCUMENT

BEST AVAILABLE COPY

出証番号 出証特 2 0 0 3 - 3 1 0 4 9 5 0

【書類名】 特許願

【整理番号】 KGA1020081

【提出日】 平成14年11月15日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 7/58

G09C 1/00

【発明者】

【住所又は居所】 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内

【氏名】 女屋 正人

【発明者】

【住所又は居所】 群馬県前橋市上佐鳥町54-2 株式会社数理設計研究所内

【氏名】 玉置 晴朗

【発明者】

【住所又は居所】 東京都台東区上野1丁目19番10号 三洋セミコンデバイス株式会社内

【氏名】 池谷 昭

【特許出願人】

【識別番号】 000001889

【氏名又は名称】 三洋電機株式会社

【特許出願人】

【識別番号】 502398610

【氏名又は名称】 株式会社数理設計研究所

【特許出願人】

【住所又は居所】 東京都台東区上野1丁目19番10号

【氏名又は名称】 三洋セミコンデバイス株式会社

## 【代理人】

【識別番号】 100075258

【弁理士】

【氏名又は名称】 吉田 研二

【電話番号】 0422-21-2340

## 【選任した代理人】

【識別番号】 100096976

【弁理士】

【氏名又は名称】 石田 純

【電話番号】 0422-21-2340

## 【手数料の表示】

【予納台帳番号】 001753

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 乱数生成装置

【特許請求の範囲】

【請求項 1】 各々所定の疑似乱数系列の乱数を出力可能な複数の疑似乱数生成手段と、

前記複数の疑似乱数生成手段の出力に基づいて出力乱数を生成可能な出力乱数生成手段と、

物理乱数を生成する物理乱数生成手段と、

前記物理乱数生成手段の生成した物理乱数に基づいて、前記出力乱数生成手段における出力乱数の生成に、少なくとも一つの前記疑似乱数生成手段で生成される疑似乱数を用いるか否かを切り替える切替手段と、

を備える乱数生成装置。

【請求項 2】 前記切替手段は、物理乱数に基づいて、少なくとも一つの前記疑似乱数生成手段にクロック信号を入力するか否かを切り替えることを特徴とする請求項 1 に記載の乱数生成装置。

【請求項 3】 前記物理乱数生成手段の生成した物理乱数が少なくとも一つの前記疑似乱数生成手段のクロック信号として入力されることを特徴とする請求項 1 に記載の乱数生成装置。

【請求項 4】 前記切替手段は、物理乱数に基づいて、少なくとも一つの前記疑似乱数生成手段で生成された疑似乱数を前記出力乱数生成手段に入力するか否かを切り替えることを特徴とする請求項 1 に記載の乱数生成装置。

【請求項 5】 前記出力乱数生成手段は、排他的論理和ゲートであることを特徴とする請求項 1 ～ 4 のうちいずれか一つに記載の乱数生成装置。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、乱数生成装置に関し、特に暗号化アルゴリズムに好適な乱数生成装置に関する。

【 0 0 0 2 】

**【従来の技術】**

暗号化アルゴリズム等では、セキュリティの確保のために、しばしば乱数が用いられる。その場合の乱数としては、一般的に、M系列 (Maximum length code : 最長符号系列) 等に代表される疑似乱数が用いられてきた。M系列符号は、公知の線形シフトレジスタ符号発生器によって生成することができる。

**【0003】**

また、上記疑似乱数以外の乱数として、原子核の崩壊現象がランダムとなることや電気雑音等の自然現象を利用して生成される物理乱数が知られている。暗号化アルゴリズム等においても、上記疑似乱数に替えて、この物理乱数を利用する場合もある (例えば、特許文献1参照。 )。

**【0004】****【特許文献1】**

特開 2000-66592号公報

**【0005】****【発明が解決しようとする課題】**

しかしながら、M系列等に代表される疑似乱数は、必ずしも安全性の高い乱数とは言えず、セキュリティ確保の面からは好ましくない面がある。疑似乱数は、一定の算術プロセスあるいは関数の組み合わせから生成されるため、同じ初期条件を与えれば、同一の乱数を生成可能となるからである。

**【0006】**

また、一般的に物理乱数は微弱な信号であるため、暗号化アルゴリズム等で使用するためには、通常、増幅器によって利用可能なレベルに増幅される。ところが、増幅器は電界や磁界によって影響を受ける場合があり、それらの意図的な印加によって乱数の発生確率が操作され、安全性が低下してしまう場合があった。

**【0007】****【課題を解決するための手段】**

本発明にかかる乱数生成装置は、各々所定の疑似乱数系列の乱数を出力可能な複数の疑似乱数生成手段と、上記複数の疑似乱数生成手段の出力に基づいて出力乱数を生成可能な出力乱数生成手段と、物理乱数を生成する物理乱数生成手段と

、上記物理乱数生成手段の生成した物理乱数に基づいて、上記出力乱数生成手段における出力乱数の生成に、少なくとも一つの上記疑似乱数生成手段で生成される疑似乱数を用いるか否かを切り替える切替手段と、を備える。すなわち、上記本発明にかかる乱数生成装置によれば、複数の疑似乱数系列のうち出力乱数の元となる疑似乱数系列が物理乱数に基づいて変更されるため、従来の疑似乱数のみを用いた乱数生成装置に比べて乱数の予測性を低減することができる。また、物理乱数を直接的な出力乱数としては用いないため、仮に外部から物理乱数生成手段に何らかの操作が加えられたとしても、出力乱数の予測は従来装置に比べてかなり難しくなる。

#### 【0008】

上記本発明にかかる乱数生成装置では、上記切替手段が、物理乱数に基づいて、少なくとも一つの上記疑似乱数生成手段にクロック信号を入力するか否かを切り替えるように構成してもよい。この構成では、疑似乱数生成手段にクロック信号を入力するか否かを切り替えることで、その疑似乱数生成手段から新たな疑似乱数が出力されるか否かが切り替わる。

#### 【0009】

また、上記本発明にかかる乱数生成装置では、上記物理乱数生成手段の生成した物理乱数が少なくとも一つの上記疑似乱数生成手段のクロック信号として入力されるように構成してもよい。この構成では、クロック信号としての物理乱数出力の値が切り替わることで、その疑似乱数生成手段から新たな疑似乱数が出力されるか否かが切り替わる。なお、この場合には、上記物理乱数生成手段が上記切替手段として機能することになる。

#### 【0010】

また、上記本発明にかかる乱数生成装置では、上記切替手段が、物理乱数に基づいて、少なくとも一つの上記疑似乱数生成手段で生成された疑似乱数を上記出力乱数生成手段に入力するか否かを切り替えるように構成してもよい。この構成では、切替手段によって、少なくとも一つの疑似乱数生成手段によって生成された疑似乱数を出力乱数生成手段に入力するか否かを切り替える。

#### 【0011】

**【発明の実施の形態】**

実施の形態1. 図1は、本実施形態にかかる乱数生成装置10の構成を示す図、また図2は、物理乱数発生器16の構成図である。

**【0012】**

乱数生成装置10は、二つの疑似乱数生成部12a, 12b、出力乱数生成部14、物理乱数発生器16、および切替部18を含む。このうち疑似乱数生成部12a, 12bは、それぞれ、縦続して接続された複数のフリップフロップを含むシフトレジスタ20a, 20bと、所定の複数のタップ位置からの出力値の排他的論理和を出力するEXORゲート22a, 22bと、を有し、所定のM系列の乱数を出力する線形シフトレジスタ符号発生器として構成されている。図1の例では、シフトレジスタ20aは、17個のフリップフロップを有しクロック信号に応じてビットシフトする17段シフトレジスタであり、入力側より第3番目と第17番目のフリップフロップからのタップ出力(Q出力; Q3, Q17)に基づいて帰還入力値(シフトレジスタ20aのD1入力; 「1」(ハイレベル)または「0」(ローレベル))が生成される。また、シフトレジスタ20bは、15個のフリップフロップを有しクロック信号に応じてビットシフトする15段シフトレジスタであり、入力側より第2番目と第15番目のフリップフロップからのタップ出力(Q2, Q15)に基づいて帰還入力値が生成される。シフトレジスタ20a, 20bの段数および帰還入力の元となるタップ位置は互いに異なっており、疑似乱数生成部12a, 12bは、相異なるM系列符号を生成することができる。

**【0013】**

本実施形態では、疑似乱数生成部12aが動作するためのクロック信号(シフトレジスタ20aがビットシフトを行うためのクロック信号)は、信号源24より直接入力されるが、疑似乱数生成部12b(シフトレジスタ20b)のクロック信号は、信号源24より切替部18を介して入力される。切替部18は、物理乱数発生器16からの物理乱数出力に基づいて、疑似乱数生成部12bにクロック信号を入力するか否かを切り替える。図1の例では、切替部18はANDゲートとして構成され、信号源24からの共通クロック信号の値が「1」であり、か

つ物理乱数出力値が「1」であるときにのみ、疑似乱数生成部12bに☐入力するクロック信号の値（すなわち出力値）を「1」とする。疑似乱数生成部12bは、☐入力されるクロック信号の値が「1」（ハイレベル）であるときにのみ新たな疑似乱数を出力する（疑似乱数を更新する）から、疑似乱数生成部12bで生成された疑似乱数は物理乱数出力値が「1」であるときにのみ出力乱数生成部14に入力され、他方、物理乱数出力値が「0」であるときは、その出力値は出力線につながるビットの値（図1の例では第15番目のビットのQ15出力；「1」または「0」）で固定されることとなる。

#### 【0014】

そして、出力乱数生成部14において、二つの疑似乱数生成部12a, 12bの出力値に基づいて出力乱数が生成される。図1の例では、出力乱数生成部14は、EXORゲートとして構成され、疑似乱数生成部12a, 12bからの出力値が不一致であるときには出力値を「1」とし、他方、それらが一致するときには出力値を「0」とする。ここで、上述したように、物理乱数出力値が「1」であるときは、疑似乱数生成部12bの出力値は疑似乱数となり、他方、物理乱数出力値が「0」であるときは、疑似乱数生成部12bの出力値は「1」または「0」で固定される。つまり、出力乱数生成部14の出力乱数は、物理乱数出力値が「1」であるときは、疑似乱数生成部12a, 12bの双方で生成された疑似乱数に基づいて生成されることとなり、物理乱数出力値が「0」であるときは、疑似乱数生成部12aによって生成された疑似乱数に基づいて生成されることとなる。すなわち、本実施形態によれば、出力乱数をどの疑似乱数を用いて生成するかが物理乱数によってランダムに変化することとなり、従来の物理乱数あるいは疑似乱数に比べて、その予測が非常に難しくなると言える。さらに、本実施形態では、複数の疑似乱数生成部12a, 12bによって相異なる疑似乱数が生成されるので、それら複数の疑似乱数生成部12a, 12bの双方に基づいて生成された出力乱数自体の予測も難しく、結果として出力乱数の予測は極めて難しくなる。

#### 【0015】

ところで、物理乱数発生器16は、物理乱数発生源16a、増幅回路16bお



よび二値化回路 16 c を備える。このうち、物理乱数発生源 16 a は、自然現象に基づいてランダムに変化する信号を生じうるものであり、例えば、上記特許文献 1 に開示されるような、接合を含む電流路に生じる雑音信号を生じる半導体素子を含むものとすることができる。なお、これには限られず、放射性物質の崩壊を利用したもの等もこの物理乱数発生源 16 a として用いることができる。物理乱数発生源 16 a にて生じた信号は、増幅回路 16 b において増幅され、さらに二値化回路 16 c において二値化処理される。二値化回路 16 c は、所定のサンプリングタイミングで、増幅された信号の振幅と所定の閾値とを比較し、例えば、増幅された信号の振幅が所定の閾値より高いときには「1」を、逆に低いときには「0」を出力する。こうして物理乱数発生器 16 により、「1」または「0」を示す所定電圧の物理乱数出力値が生成される。なお、二値化回路 16 c の閾値のレベルは任意に設定することができるが、通常は「1」および「0」の発生確率がほぼ 1 対 1 となるように設定される。なお、二値化回路 16 c において、単に、増幅された信号の振幅を所定の閾値と比較して出力信号を発生するようにしてもよい。

#### 【0016】

実施の形態 2. 図 3 は、本実施形態にかかる乱数生成装置 30 の構成を示す図である。なお、ここでは、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

#### 【0017】

上記実施の形態 1 では、疑似乱数生成部 12 b には、クロック信号として、物理乱数発生器 16 からの物理乱数出力と信号源 24 からの共通クロック信号との論理積を入力したが、本実施形態では、疑似乱数生成部 12 b へのクロック信号を、物理乱数発生器 16 からの物理乱数出力そのものとしている。本実施形態では、物理乱数発生器 16 が切替部に相当する。なお、疑似乱数生成部 12 a のクロック信号 CK は物理乱数出力とは独立して入力される。このような構成とした場合も、上記実施の形態 1 と同様の効果が得られる。すなわち、物理乱数出力値が「1」であるときには、疑似乱数生成部 12 b は、物理乱数出力の出力タイミング（＝物理乱数発生器 16 のサンプリングタイミング）で、順次、疑似乱数を

生成し、これが出力乱数生成部 14 に向けて出力される。他方、物理乱数出力値が「0」であるときには疑似乱数生成部 12b は動作せず、その出力値は出力線につながるビットの値（図 3 の例では第 15 番目のビットの Q15 出力；「1」または「0」）で固定される。すなわち、物理乱数出力値が「1」であるときは、疑似乱数生成部 12b からクロック信号に応じて疑似乱数が出力され、物理乱数出力値が「0」であるときは、疑似乱数が出力されず出力値が固定された状態となる。それら各状態において出力乱数生成部 14 から出力される出力乱数は上記実施の形態 1 と同じとなる。本実施形態でも、上記実施の形態 1 と同様に、出力乱数をどの疑似乱数を用いて生成するかが物理乱数によってランダムに変化することとなり、従来の物理乱数あるいは疑似乱数に比べて、その予測が非常に難しくなると言える。なお、物理乱数発生器 16 は、サンプリングタイミングで出力するのではなく、任意のタイミングで出力するように構成してもよい。

#### 【0018】

実施の形態 3. 図 4 は、本実施形態にかかる乱数生成装置 40 の構成を示す図である。なお、ここでは、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

#### 【0019】

本実施形態では、疑似乱数生成部 12b で生成した疑似乱数が出力乱数生成部 14 に入力されるか否かが切替部 48 によって制御される。図 4 の例では、疑似乱数生成部 12b の出力は、AND ゲートとして構成される切替部 48 を介して出力乱数生成部 14 に入力されるようになっている。そして切替部 48 において、物理乱数発生器 16 からの物理乱数出力と疑似乱数生成部 12b の出力との論理積が取得され、これが出力乱数生成部 14 に入力される。すなわち、物理乱数出力値が「1」であるときは、疑似乱数生成部 12b で生成された疑似乱数がそのまま出力乱数生成部 14 に入力され、出力乱数生成部 14 は、疑似乱数生成部 12a、12b 双方の疑似乱数の排他的論理和を取得し、これを出力乱数として出力する。他方、物理乱数出力値が「0」であるときは、出力乱数生成部 14 には「0」が入力され、出力乱数生成部 14 からは、疑似乱数生成部 12a の出力値と同じ値の出力乱数（すなわち疑似乱数生成部 12a の出力した疑似乱数）が

出力される。本実施形態でも、物理乱数出力値が「1」であるときは、疑似乱数生成部12bからクロック信号（例えば疑似乱数生成部12aと共通のクロック信号）に応じて疑似乱数が出力され、物理乱数出力値が「0」であるときは、疑似乱数が出力されず出力値が固定された状態となる。つまり、本実施形態でも、出力乱数をどの疑似乱数に基づいて生成するかが物理乱数によってランダムに変化することとなり、従来の物理乱数あるいは疑似乱数に比べて、その予測が非常に難しくなると言える。

#### 【0020】

実施の形態4. 図5は、本実施形態にかかる乱数生成装置50の構成を示す図である。なお、ここでは、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

#### 【0021】

本実施形態では、疑似乱数生成部12a, 12bでそれぞれ生成された疑似乱数が出力乱数生成部14に入力されるか否かが物理乱数出力値によって切り替わる。なお、図5の例の場合、疑似乱数生成部12a, 12bの生成した疑似乱数のうちいずれか一方が選択的に出力乱数生成部14に入力され、選択入力された疑似乱数がそのまま出力乱数生成部14の出力、すなわち乱数生成装置50の出力となっている。つまり、図5の例では、複数の疑似乱数生成部12a, 12bによってそれぞれ生成される疑似乱数パターンのうちどれを出力するかを、物理乱数によって選択的に切り替えているということもできる。具体的には、切替部58は、二つのANDゲート58a, 58bを備えており、そのうち一方のANDゲート58aには、疑似乱数生成部12aの出力と物理乱数発生器16からインバータ58cを介して物理乱数出力値が入力され、もう一方のANDゲート58bには、疑似乱数生成部12bの出力と物理乱数発生器16からの物理乱数出力値が入力される。そして、これら二つのANDゲート58a, 58bの出力が出力乱数生成部14に入力され、それらの排他的論理和が出力乱数となる。そして、この構成では、物理乱数出力値が「1」であるときは、疑似乱数生成部12bで生成された疑似乱数がそのままANDゲート58bの出力として出力乱数生成部14に入力され、他方ANDゲート58aの出力は「0」となる。すなわち

この場合、出力乱数生成部 14 からは、疑似乱数生成部 12 b の出力値と同じ値の出力乱数（すなわち疑似乱数生成部 12 b の出力した疑似乱数）が出力される。他方、物理乱数出力値が「0」であるときは、疑似乱数生成部 12 a で生成された疑似乱数がそのまま AND ゲート 58 a の出力として出力乱数生成部 14 に入力され、他方 AND ゲート 58 b の出力は「0」となる。すなわちこの場合、出力乱数生成部 14 からは、疑似乱数生成部 12 a の出力値と同じ値の出力乱数（すなわち疑似乱数生成部 12 b の出力した疑似乱数）が出力される。本実施形態でも、出力乱数をどの疑似乱数に基づいて生成するかが物理乱数によってランダムに変化することとなり、従来の物理乱数あるいは疑似乱数に比べて、その予測が非常に難しくなると言える。

#### 【0022】

以上、本発明の好適な実施形態について説明したが、本発明は上記実施形態には限定されず、種々の等価回路によっても実施可能である。例えば、上記実施形態では、疑似乱数が、17 段または 15 段のシフトレジスタを有する線形シフトレジスタ符号発生器によって生成される数種類の M 系列符号である場合を例示したが、この例には限定されず、それ以外の段数のシフトレジスタあるいはタップの組み合わせに基づく疑似乱数系列であってもよい。また、複数の疑似乱数生成部を、同じ系列の疑似乱数を発生させるものとしてもよい。また、上記実施形態では、シフトレジスタの最終段のフリップフロップの Q 出力を疑似乱数として出力したが、他のフリップフロップから疑似乱数を出力してもよいし、シフトレジスタに入力される帰還値を疑似乱数出力としてもよい。

#### 【0023】

##### 【発明の効果】

以上説明したように、本発明によれば、出力乱数をどの疑似乱数に基づいて生成するかが物理乱数に基づいてランダムに変化するため、その予測が難しく暗号化アルゴリズム等への適用に際してより安全性の高い乱数を生成することができる。

##### 【図面の簡単な説明】

【図 1】 本発明の実施の形態 1 にかかる乱数生成装置の構成図である。

【図 2】 本発明の実施の形態にかかる乱数生成装置で用いられる物理乱数発生器の構成図である。

【図 3】 本発明の実施の形態 2 にかかる乱数生成装置の構成図である。

【図 4】 本発明の実施の形態 3 にかかる乱数生成装置の構成図である。

【図 5】 本発明の実施の形態 4 にかかる乱数生成装置の構成図である。

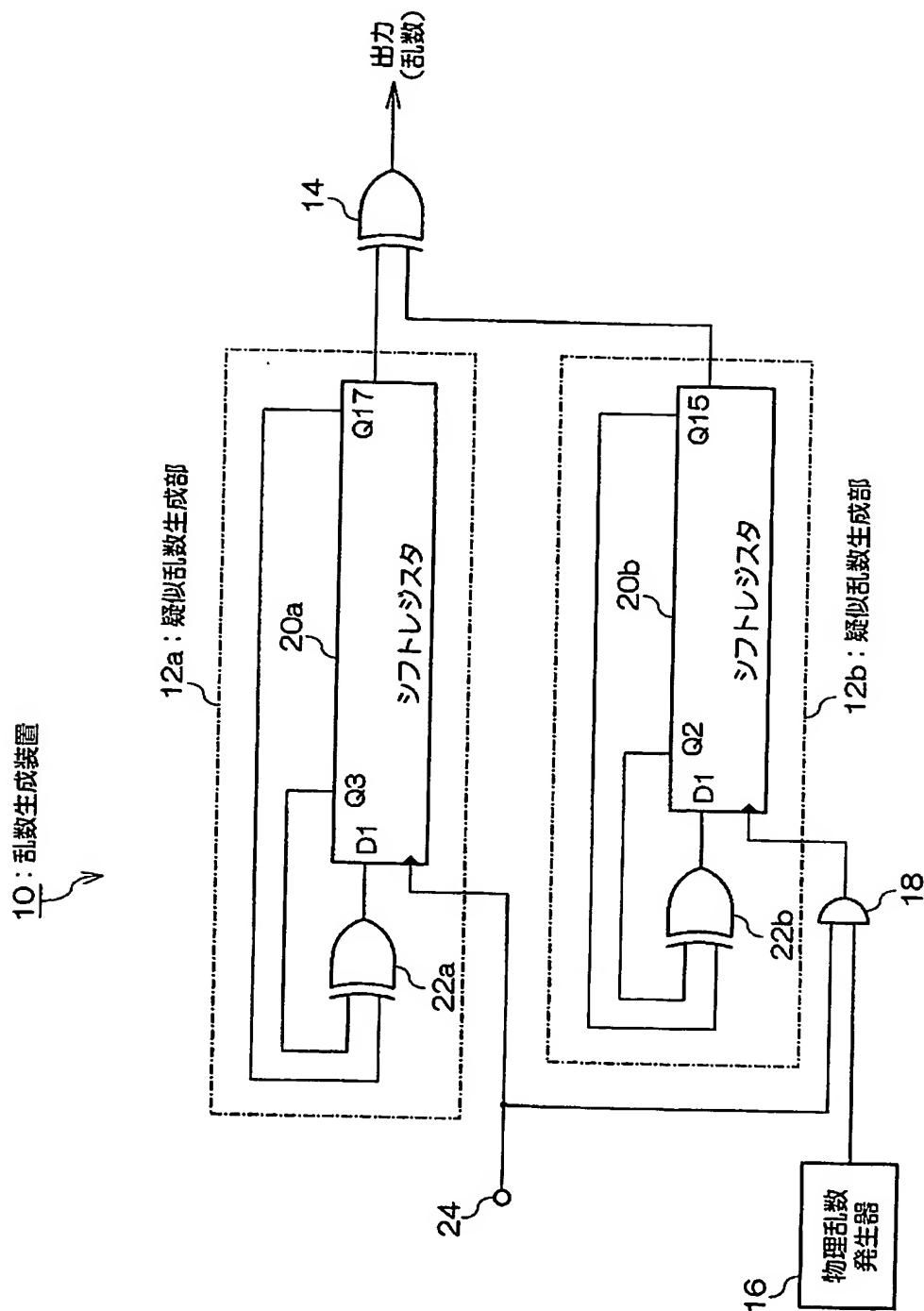
【符号の説明】

10, 30, 40, 50 乱数生成装置、12a, 12b 疑似乱数生成部、  
14 出力乱数生成部、16 物理乱数発生器、18, 48, 58 切替部、20a, 20b シフトレジスタ、22a, 22b EXORゲート、24 信号源。

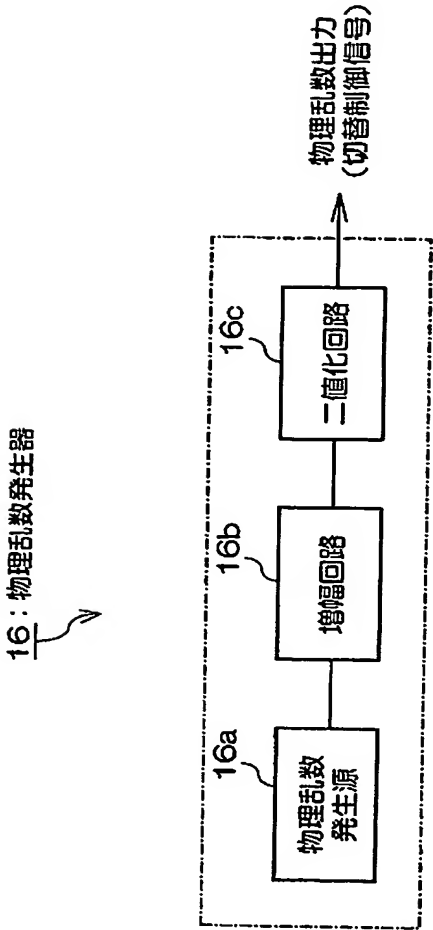
【書類名】

図面

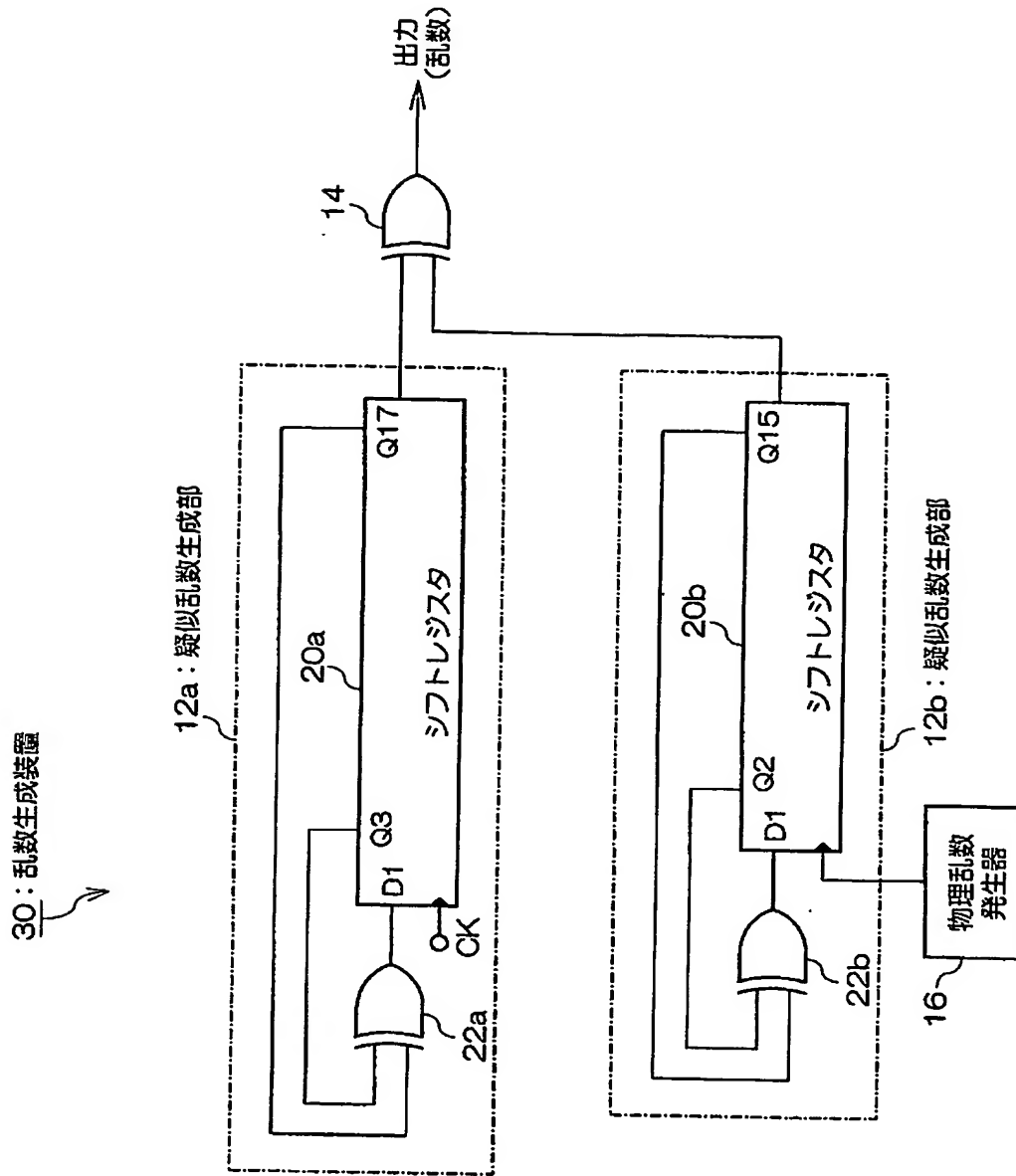
【図 1】



【図 2】

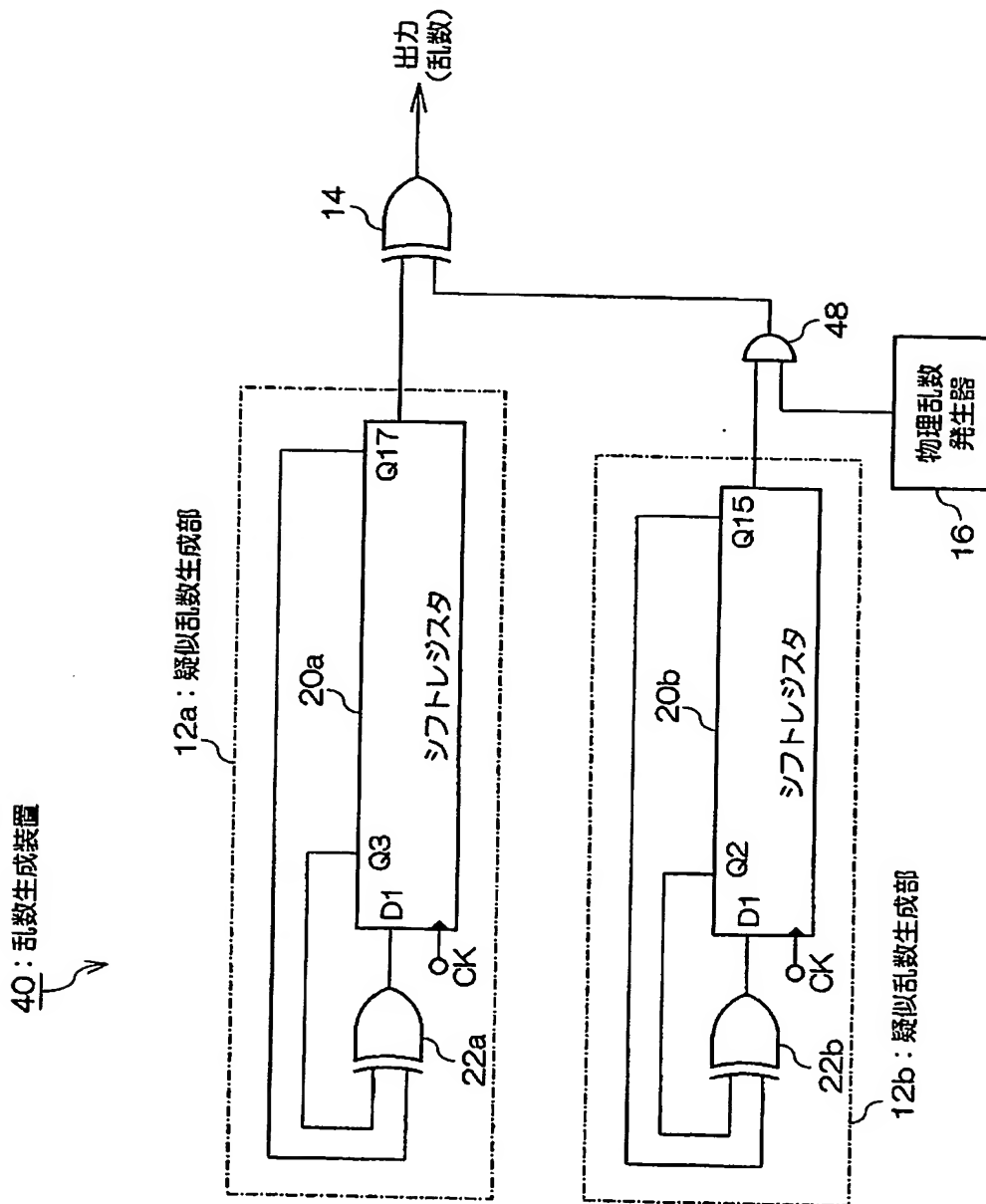


【図 3】

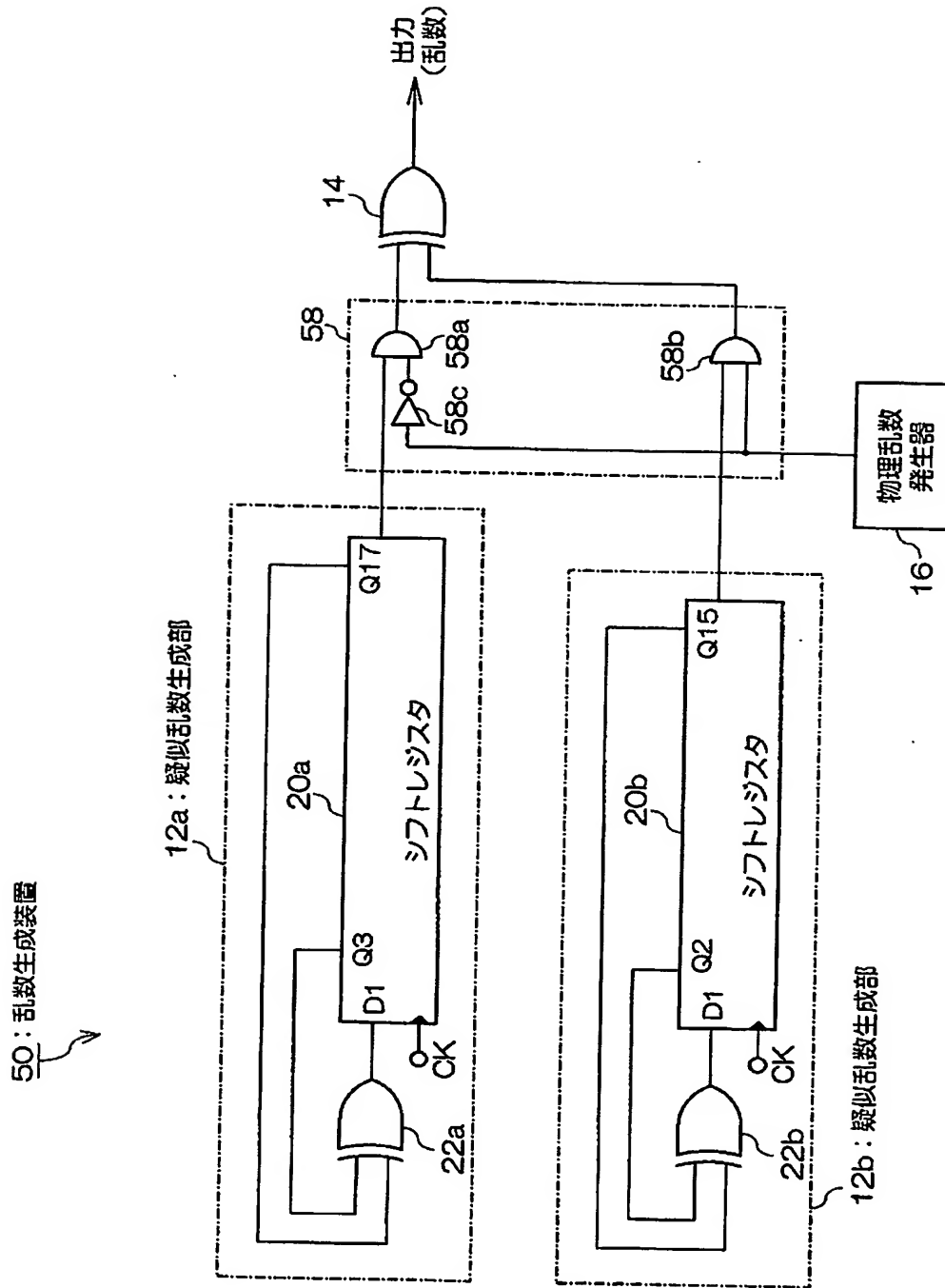




【図 4】



【図 5】



【書類名】 要約書

【要約】

【課題】 予測が困難であり、暗号化アルゴリズム等での適用についてより安全性の高い乱数を生成する。

【解決手段】 乱数生成装置 10 は、各々所定の疑似乱数系列の乱数を出力可能な複数の疑似乱数生成部 12 a, 12 b と、複数の疑似乱数生成部 12 a, 12 b の出力に基づいて出力乱数を生成する出力乱数生成部 14 と、物理乱数を生成する物理乱数発生器 16 と、物理乱数発生器 16 の生成した物理乱数に基づいて疑似乱数生成部 12 b の出力値の更新の有無を切り替える切替部 18 と、を備える。かかる構成によれば、出力乱数をどの疑似乱数系列に基づいて生成するかが物理乱数に基づいてランダムに切り替わることとなり、従来の乱数に比べ、その予測が非常に難しくなる。

【選択図】 図 1

特願 2002-331884

出 願 人 履 歴 情 報

識別番号

[000001889]

1. 変更年月日  
[変更理由]  
住 所  
氏 名

1993年10月20日  
住所変更  
大阪府守口市京阪本通2丁目5番5号  
三洋電機株式会社

特願 2 0 0 2 - 3 3 1 8 8 4

出 願 人 履 歷 情 報

識別番号

[ 5 0 2 3 9 8 6 1 0 ]

1. 変更年月日

2 0 0 2 年 1 1 月 1 日

[変更理由]

新規登録

住 所

群馬県前橋市上佐鳥町 5 4 - 2

氏 名

株式会社数理設計研究所

特願 2002-331884

出 願 人 履 歴 情 報

識別番号

[502343458]

1. 変更年月日

2002年 9月20日

[変更理由]

新規登録

住 所

東京都台東区上野1丁目19番10号

氏 名

三洋セミコンデバイス株式会社